



Interreg



EUROPEAN UNION

Danube Transnational Programme DIONYSUS

**Integrating Danube Region into Smart & Sustainable
Multi-modal & Intermodal Transport Chains**

Yearly Activity Report 2022

Version: 1.0

Date: 28.10.2022

FINAL

D.T2.4.2_DIONYSUS_Yearly
Activity Report_FINAL

Document History

Version	Date	Authorised
0.1	31.03.2022	PDM
0.2	02.05.2022	PDM
0.3	29.07.2022	PDM
0.4	18.10.2022	PDM
1.0	28.10.2022	PDM

Contributing Authors

Name	Organisation	Email
Robert Rafael	PDM	rafael@prodanube.eu
Ruxandra Matzalik Florescu	PDM	florescu@prodanube.eu
Christian Stark	PDM	stark@prodanube.eu
Markus Eppich	PDM	eppich@prodanube.eu
Werner Auer	EHOÖ	w.auer@ennshafen.at
Cristiana Dima	MPAC	CDima@constantza-port.ro
PP experts (assigned Communication experts)	All DIONYSUS partners	

1 Table of Contents

1	Table of Contents.....	2
2	Abbreviations.....	3
3	Introduction.....	4
4	Revision of the RIS Directive	5
5	Importance of cybersecurity in the digital age	6
5.1	Cybersecurity & IWT	6
5.2	The cybersecurity regulatory framework.....	7
5.2.1	The Network Information Security Directive.....	7
5.2.2	The EU Cybersecurity Act	8
6	Relevant project results	9
6.1	EuRIS.....	9
6.2	CEERIS.....	9
6.3	Danube FIS Portal.....	10
6.4	WAMOS.....	10
7	List of projects	11
8	Literature	15

2 Abbreviations

Abbreviation	Explanation
CESNI	European Committee for Drawing UP Standards in the Field of Inland Navigation
CEERIS	Central & Eastern European Reporting Information System
DPN	Danube Ports Network
EC	European Commission
EU	European Union
EuRIS	European River Information Services
IWT	Inland Waterway Transport
PDM	Pro Danube Management GmbH
RIS	River Information Services

3 Introduction

The aim of the third and final of a series of 3 Yearly Activity Reports elaborated in the frame of **WP T2 Danube Inland & Sea Ports Analysis & Recommendations, A.T2.4 Danube Port Digitization (Strategy & Action Plan)**, is to discuss and identify digitalisation initiatives along the logistics chains in line with RIS deployments and to present EU digitalisation policy goals, legislation and measures that have an immediate impact on IWT.

Given that the previous 2 yearly activity reports already provided a comprehensive policy analysis on the specific European legislation impacting the digitalisation process of IWT, the present document shall, in a first step, update on the ongoing revision process of the RIS Directive. An equally important topic – cybersecurity – shall also be discussed. Given that digitalisation in terms of the development of new technologies is expected to fundamentally change inland shipping, whereas fully or semi-automated operations are expected to streamline daily activities, this process is not without some downsides, such as the exposure of data or information to hackers. This deliverable therefore argues that IWT's challenging pathway towards digitalisation must put cybersecurity high on its agenda, providing a brief and concise policy analysis on the European legislative framework shaping cybersecurity. The sixth chapter of this deliverable discusses 3 important applications elaborated in the frame of transnational projects, all of which are essential in IWT's digitalisation process: the EuRIS and the CEERIS applications elaborated in the frame of RIS COMEX and WAMOS elaborated in the frame of the FAIRway projects. The final chapter lists several EU funded projects dealing with digitalisation in IWT – covering several aspects such as physical internet and smart multimodal logistics. The Digital Initiatives Observatory, hosted by the website of the Danube Ports Network (DPN), will be updated with the information collected in this report.

4 Revision of the RIS Directive

River Information Services (RIS) are modern traffic management systems enhancing a swift electronic data transfer between water and shore through in-advance and real-time exchange of information. These services are designed to enhance safety and efficiency of IWT by optimising traffic and transport processes. Focal aspect is a swift demand oriented electronic data transfer between water and shore through a real-time exchange of information. As such, RIS aims to streamline the exchange of information between IWT stakeholders. The 2005 adopted RIS Directive provides minimum requirements for the implementation of RIS and its agreed standards in order to enable the cross-border compatibility of national systems, functioning as the main pillar of digitalisation in IWT.

Mid-2021, the Commission released the Inception Impact Assessment (Roadmap) for the revision of Directive 2005/44/EC on harmonised river information services which aims to inform citizens and stakeholders about the Commission's plans in order to allow them to provide feedback on the intended initiative and to participate effectively in future consultation activities. One year into the revision, the raised discussions and collected input went around subjects such as the difference in scope of eFTI and RIS, personal data protection, the need for having additional guidelines, the incorporation of CESNI in the process for creating and adopting RIS technical specifications, and the difficulty in making an electronic reporting obligation on EU level. The evaluation confirmed the relevance of RIS, highlighting that specific improvements which refer to the degree of harmonisation, reduction of administrative burden as well as an improved adoption process of technical standards are of utmost importance, whereas new challenges in particular areas of digitalisation, environment and transport connectivity still need to be adequately tackled.

The initiative to revise the RIS Directive is in line with the key objectives enshrined in the European Green Deal which stipulates that a substantial part of the 75% of inland freight carried today by road should shift onto rail and inland waterways, the Sustainable and Smart Mobility Strategy which highlights the urgent need for the use of more sustainable transport modes, indicating that inland waterway transport and short-sea shipping should increase by 25% by 2030 and by 50% in 2050. A detailed analyses and an evaluation of the legislation governing digitalisation in IWT was carried out in the frame of the Yearly Activity Report 2021.

The revision of the RIS Directive is according to the NAIADES3 action plan envisaged to be completed in 2022.

5 Importance of cybersecurity in the digital age

The aim of this chapter is to provide a concise analysis of the current role and status of cybersecurity in the ongoing digitalisation process of IWT. Given the ambitious climate goals of the European Union and the ongoing trend of globalisation, the process of digitalisation within the IWT sector will undoubtedly be further accelerated. The advantages of digitalisation are obvious: it streamlines processes, increases productivity and efficiency, reduces operational and administrative costs, and improves the competitive advantage – just to name a few. However, the process of digitalisation is not without some downsides such as the exposure of information to hackers. Digitalisation in IWT therefore must regard cybersecurity as a fundamental prerequisite to its successful implementation.

In a global and digitalised world, cybersecurity has become in many ways a race between defenders and attackers. Attackers constantly analyse the weaknesses of IT systems forcing defenders to have a watchful eye on any potential threats. A successful cyberattack might compromise the privacy, integrity and even availability of an ICT (**I**nformation and **C**ommunication **T**echnology) system. Inadequate cybersecurity measures can lead to numerous harmful consequences such as obtaining financial, personal, or professional information without the knowledge of the victim. So-called Denial-of-Service (DoS) attacks can slow down or even prevent access of the legitimate users to computer systems. Attacks on industrial control systems can lead to the destruction or disruption of the equipment which controls them (Mihai/Ciuchi/Petrica 2018: 25).

5.1 Cybersecurity & IWT

Published in 2019, the PIANC **“Awareness Paper on Cybersecurity in Inland Navigation”** is to date the most comprehensive study published on cybersecurity aspects in IWT. The document highlights the fact that even though cybersecurity is intensively researched and high on the agenda within other industries, in IWT it rather seems to be a neglected issue (PIANC 2019: 9). Not much has changed since then. The study lists the systems currently in use that might be potential targets of cyberattack. These are, but are not limited to, the following (PIANC 2019: 9):

On-board systems (by function):

- Vessel control, e.g.
 - Propulsion and machinery management,
 - Power control systems.
 - Wheelhouse systems, including devices for elevating wheelhouses,
 - Fuel, battery and cargo handling;
- Navigation, e.g.
 - Vessel Tracking and Tracing (VTT) Standard for Inland Navigation (Inland AIS),

- Electronic Chart Display and Information System for Inland Navigation (Inland ECDIS),
- Radar,
- Electronic Ship Reporting in Inland Navigation (ERI),
- Notices to Skippers for Inland Navigation (NtS);
- Infrastructure Control Systems
 - Lock and bridge management (LBM),
 - Traffic planning,
 - Aids to navigate that rely on information technology;
- Information reporting/exchange, e.g. systems concerned with:
 - ITL – Information for Transport Logistics,
 - ILE – Information for Law Enforcement,
 - Cargo and fleet management (CFM) including information about dangerous cargo;
- Network Infrastructure/communication systems, e.g:
 - Bespoke industry web portals,
 - Distributed devices.

Most of these items fall under the category RIS (River Information Services).

As highlighted by PIANC's recent report **“Smart Shipping on Inland Waterways”**, smart shipping is highly data driven, therefore aspects of privacy and security become very important. Security breaches must be avoided (PIANC 2022: 32).

Equally important to highlight are the ongoing proceedings with regard to cybersecurity by the CCNR. More detailed information and presentations on the current status of cybersecurity in IWT is available here: <https://www.ccr-zkr.org/13020152-en.html>.

5.2 The cybersecurity regulatory framework

Two key pillars shape the European cybersecurity policy landscape - namely the **Network Information Security Directive** and the **Cybersecurity Act**. Both are quite young – while the Network Information Security Directive came into effect in 2018, the Cybersecurity Act was enacted in 2019. The following subchapters aim to provide a brief overview on both pieces of legislation.

5.2.1 The Network Information Security Directive

The directive regulates “the measures with a view to achieving a **high common level of security of network and information systems within the Union** so as to improve the functioning of the internal market”. Within the context of this Directive, “security of network and information systems” is regarded as “the ability of network and information systems to resist, at a given level of confidence, any action that

compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems” (Art. 4 (2)).

This piece of legislation is the **first cybersecurity legislation adopted at European level** which has a direct impact on each and every member state, with EU legislation having precedence over the national one.

5.2.2 The EU Cybersecurity Act

One of the most important elements of the new act refers to a new permanent and enhanced mandate for ENISA – the European Union Agency for Cybersecurity. Equally important to highlight is the adoption of a new Pan-European **Cybersecurity Certification Scheme**. This means that those who want to get certified have now access to a one-stop shop in several member states, contributing this way to a higher degree of harmonisation as already initiated by the NIS Directive. These schemes refer to ICT (**I**nformation and **C**ommunications **T**echnology) products, services, and processes. For now, the schemes are voluntary, with the European Cybersecurity Act granting a probation time of 4 years – until 31 December 2023. After that, the European Commission shall assess whether certain schemes should become mandatory (Art. 56). Generally speaking, the aim of the EU Cybersecurity Act is to increase the quality of EU products and services by guaranteeing a high level of cybersecurity.

6 Relevant project results

The aim of this chapter is to provide a brief overview on the most promising developments in several projects closely linked to the digitalisation process of IWT.

6.1 EuRIS

Developed within the RIS COMEX project, EuRIS gives easy access to all information you need as a skipper, vessel owner or logistic operator on the main European waterways. You can register your vessels and follow their route, receive a message when one of your vessels passes a certain point on the network and request information on vessels, voyages and cargo. And there are many more possibilities. As the owner of the information, you are always in charge of who is allowed to see which information.

EuRIS presents all waterway and traffic related information of thirteen European countries on handy maps or in tables, with

- a real-time traffic image,
- position information of authorized vessels,
- Notices to Skippers,
- actual water levels, discharges, bridge clearance, water depth,
- information about the fairways, bridges, locks, berths, terminals,
- the operating times of locks and bridges,
- a Route and Voyage Planner,
- travel duration and expected arrival times.

The portal is currently in a preview phase and is subject to improvements regarding data coverage, completeness, and usability. The portal is available here: <https://www.eurisportal.eu/>.

6.2 CEERIS

CEERIS stands for “**Central & Eastern European Reporting Information System**” and is a joint initiative of 8 countries: Austria, Bulgaria, Croatia, Czech Republic, Hungary, Romania, Serbia and Slovakia. The platform enables vessel operators navigating in the Danube corridor and the Elbe River in Czech Republic to fulfil all reporting requirements for a specific inland waterway transport in participating countries by “reporting only once” with “single entering of data”. CEERIS and EuRIS share various services as user management, vessel position provision, ETA and voyage calculation as well as ERI data exchange to profit from each other to the advantage of their users.¹

The portal can be accessed here: www.ceeris.eu.

¹ www.ceeris.eu

6.3 Danube FIS Portal

The Danube FIS Portal was set up in the project NEWADA and further developed in its successor project NEWADA duo (both co-financed by the EU SEE Transnational Cooperation Programme). The project Danube STREAM (co-funded by the European Union (ERDF, IPA)) took up the Danube FIS portal and improved its functionalities and user interface until 2019.

Details are available here: <https://www.danubeportal.com/>

6.4 WAMOS

Several Danube riparian countries have taken a first step towards unifying and merging national waterway data into a transnational Waterway Monitoring System (WAMOS). This web application, developed within the FAIRway project, collects hydrological and hydrographical data from the Danube Waterway Administrations into one system. WAMOS offers a harmonised display and analysis of the data, being available to registered users only (waterway administrations). Within the ongoing proceedings of *Preparing FAIRway 2*, functional upgrades of WAMOS are envisaged. The new functionalities of WAMOS 2.0 are intended to improve the system's analytical capabilities, user friendliness and efficiency of operations for all users by simplification and automation of processes. The plan is for WAMOS 2.0 to integrate new data linked to the physical status of the waterway such as bridge clearance, discharge or AIS Aids to Navigation. Merging these data with traffic analysis allows a better understanding of a specific use of a waterway, in particular in shallow water areas or narrow sections. Moreover, the upgraded version of WAMOS will enable an effective monitoring of rehabilitation and maintenance measures. WAMOS currently uses data from different sources such as the D4D-Portal, national WAMS (Waterway Asset Management System), or River Information Services (RIS). For the future development of the application, new sources of data are being considered – such as the newly developed EuRIS system developed in the frame of the RIS COMEX project.²

² Preparing FAIRway 2 works in the Rhine-Danube-Corridor Newsletter March 2022

7 List of projects

This chapter provides a list of identified projects dealing with digitalisation in IWT and was developed to complete the list developed in the previous two editions of the **Yearly Activity Report**. This list of projects is considered a “living document” and will be made available via the e-tool “**Digital Initiatives Observatory**” hosted by the website of the Danube Ports Network (www.danubeports.eu). The list of projects will continuously be updated until the end of DIONYSUS.

Project name: **Resilience-centric Smart, Green, Networked EU Inland Waterways**

Abbreviation: **ReNEW**

Funding programme: **Horizon Europe**

Timeframe: **2022-2025**

Coordinator: **European Inland Waterway Transport (IWT) Platform**

Website: <https://cordis.europa.eu/project/id/101069682>

ReNEW represents a multidisciplinary group composed of 24 participants from 11 countries of the European Union capable of playing a key role in supporting the transition of IWT to smart, green, sustainable and climate-resilient sector. To achieve this, the project will build on previous results, will capitalise on cooperation opportunities with ongoing projects and initiatives and will deliver:

- An interdisciplinary IWT Resilience and Sustainability decision-support framework incorporating innovative models for IWT infrastructure networking interdependencies linking to probabilistic risk and safety analyses and resilience quantification (Resilience Index), supporting the identification of short- and long-term measures that enhance resilience utilising SOA building blocks from Reference Projects
- Targeted innovative infrastructure resilience and sustainability solutions building on autonomy developments and maturing green energy options;
- A Green Resilient IWT Dataspace and generic Digital Twin providing primarily data sharing between infrastructure monitoring, RIS and traffic management and emergency systems and climate solutions;
- Four Living Labs designed to provide exemplars from a) LLs focusing on integrated IW and hinterland infrastructure [Gent-urban, Douro- corridor, Netherlands – EU network perspectives] and a LL addressing specifically inland waterway resilience;
- ReNEW Outreach and Upscale activities designed to maximise impact pathways.

Project name: **Climate resilient and environmentally sustainable transport infrastructure, with a focus on inland waterways**

Abbreviation: **CRISTAL**

Funding programme: **Horizon Europe**

Timeframe: **2022-2025**

Coordinator: **SIEC BADAWCZA LUKASIEWICZ - POZNANSKI INSTYTUT TECHNOLOGICZNY, Poland**

It is the key objective of the project CRISTAL (36 months) to increase the share of freight transport on inland water transport (IWT) by a minimum of 20% and to demonstrate on its three pilot sites (Italy, Poland and France) strategies to improve reliability by 80%.

CRISTAL project will assure IWT capacity at 50% even during extreme weather events. Towards that CRISTAL will co-create, test and implement integrated, cooperative and innovative solutions in its three pilot partners' areas identified in Italy, France and Poland. The project will include the aspects of technological innovation/development and digitalization; further advancement towards the Physical Internet, governance solution and business models, will be proposed while targeting sustainability and infrastructure resilience requirements.

Project name: **Open collaboration and open Digital Twin infrastructure for Green Smart Shipping**

Abbreviation: DT4GS

Funding programme: **Horizon Europe**

Timeframe: **2022-2025**

Coordinator: **Inlecom Group, Belgium**

DT4GS is aimed at delivering an “Open Digital Twin Framework” for both shipping companies and the broader waterborne industry actors to tap into new opportunities made available using Digital Twins (DTs). The project will enable shipping stakeholders to embrace the full spectrum of DT innovations to support smart green shipping in the upgrade of existing ships and new vessels. DT4GS will cover the full ship lifecycle by embracing federation of DT applications as well as utilising DTLF policies and related shared-dataspace developments for the sector. DT4GS applications will focus on shipping companies but will also provide decarbonisation decision-support system for shipyards, equipment manufacturers, port authorities and operators, river commissions, classification societies, energy companies and transport/corridor infrastructure companies. DT4GS's objectives are to:

- Support shipping companies in achieving up to 20% reduction in CO₂e with a 2026 horizon, by developing and deploying real-time configurable DTs for ship and fleet operational performance optimisation in 4 Living Labs involving shipping companies, with different vessel types, and establishing fully validated

industry services for Green Shipping Operational Optimisation DTs expected to be adopted by 1000+ ships by 2030.

- Establish a comprehensive zero-emission shipping methodology and support Virtual Testbed and Decision Support Systems that address both new builds and retrofits comprising:
 - A DT4GS (Green Shipping) Dataspace for the broader shipping sector contributing to GAIA-X by establishing a core European industry resource that accelerates the green and digital transition of waterborne shipping and transport value chains.
 - Simulation based solutions to retrofit ships, targeting 55% reduced CO₂e reduction by 2030.
 - A smart green “new-build” reference design per vessel type.
 - Virtual Testbed services for reducing the cost of physical testing of GS solutions by 20%.

Project name: **Port solutions for efficient, effective and sustainable multimodality**

Abbreviation: **MultIRELOAD**

Funding programme: **Horizon Europe**

Timeframe: **2022-2025**

Coordinator: **Duisburger Hafen Aktiengesellschaft, Germany**

MultIRELOAD focusses on the specific role and challenges of inland ports as multimodal freight nodes in reaching Europe’s greenhouse gas (GHG) reduction target of at least 55 % by 2030, thereby shifting a substantial part of the 75% of inland freight carried today by road in the EU to inland waterways and rail, and by increasing operational efficiency, safety and reliability of existing infrastructures through digitalization. Inland Ports are key for multimodal transport chains, both continental and maritime transport. Without efficient nodes in the hinterland multimodal transport is not possible. However, the constraints and barriers are much higher in inland ports (space, urbanisation, demand, investments) than in seaports. MultIRELOAD enhances the collaboration between different freight nodes in Europe to jointly test innovations and create favorable market conditions for multimodal freight transport solutions. MultIRELOAD will demonstrate solutions in three Innovation Areas with specific aims by 2025 – mirroring measures of the EU’s Smart Mobility Strategy: A) Smart multimodal logistics: facilitate a shift from road to rail & IWT of 5%; B) Digital & Automated Multimodal Nodes and Corridors: increase operational efficiency by 20 % raise of handling capacity; C) Innovative business models: leading to an average cost reduction of freight transport by 10%. MultIRELOAD involves highly ambitious logistics hubs, including the multimodal node duisport (DE), Duisburg's highly ambitious port and the world’s largest and most advanced trimodal inland hub terminal, and the trimodal nodes Ports of Vienna (AT) and Basel (CH). The project is backed up by additional funding & financing for better integration of the freight transport nodes into overall logistic chains of about 450 Mio. EUR. MultIRELOAD involves a total of 22 partners comprising of highly innovative

technology, logistics and service providers, leading European research institutions and well-connected networks.

Project name: **Sustainability EducationAI programme for greeNEr fuels and enerGY on ports**

Abbreviation: **SEANERGY**

Funding programme: **Horizon Europe**

Timeframe: **2022-2025**

Coordinator: **MAGELLAN CIRCLE - EUROPEAN AFFAIRS CONSULTANCY, LDA**

Contributing to reach the European Green Deal objectives and the Europe 2050's goals, the SEANERGY Project aims to provide a solution for exploiting the untapped potential of EU-ports energy's system by implementing the SEANERGY Master Plan which assesses stakeholders to execute the necessary activities towards transforming ports, regardless of their geographical context, into active members of the clean energy and fuel generation grid of EEZ. Activities such as training, reskilling, awareness spreading and communication channels creation, will set the basis of the green port transitioning, creating spaces of dialogue and teaching among all agents of the industry (private and public), which will, in turn, boost the development and integration of these technologies, along with prepared professionals that will be able to manage and implement them promptly, securely and efficiently. The SEANERGY project will be developed in 3 stages: (1) understanding of actors and port E&F systems and identifying limitations; (2) developing the Master Plan and Handbook, which will serve as a training manual for stakeholders, as well as implementing the Industry-Academy programme to train future professionals in clean energy technologies and fuels and how to apply the knowledge in ports; (3) expanding the scope of the Master Plan beyond Europe.

8 Literature

Mihai, Ioan-Cosmin/Ciuchi, Costel, Petrica, Gabriel (2018). Provocari actuale in domeniul securitatii cibernetice – impact si contributia Romaniei in domeniu (Challenges in cybersecurity – impact and contribution of Romania). Institutul European din Romania.

PIANC - Awareness Paper on Cybersecurity in Inland Navigation (2019).

PIANC – Smart Shipping on inland waterways (2022).